Claims

1. In a network controlled by an enterprise but having at least one link for establishing a connection to a network not controlled by the enterprise, comprising:

a plurality of sub-networks, wherein

each sub-network *i* includes at least one processing unit,

at least one processing unit of at least one of said plurality of sub-networks is a periphery switch of said network and is connectable to one or more other networks that are not controlled by said enterprise, and

each sub-network *i* employs N_i links, N_i being an integer greater than 0, for communication between said at least one processing unit and one of another processing unit within a common sub-network, a processing unit within another sub-network of the network controlled by the enterprise, and

a firedoor module *i*, associated with said N_i links, that includes means to block effects of all known malfeasing data addressed to flow through said N_i links of said sub-network *i*.

2. The arrangement of claim **1** where said firedoor module *i* is further selectively adapted to block traffic seeking to flow out of said sub-network, out of said network *i*, or both in and out of said network *i* when said firedoor module *i* concludes that a likelihood exists that malfeasing data aims to flow out of said sub-network *i*.

3. The arrangement of claim **1** where more than one of said N_i links is connected to one of said one or more periphery elements of said sub-network *i*.

4. The arrangement of claim **1** where said N_i links are grouped into *J* groups, each group associated with a different one of said periphery elements, said firedoor module *i* consists of *J* submodules, each associated with a different group of said N_i links, and at least one of said submodules comprises a plurality of firedoor elements, each associated with one of said N_i links.

5. The arrangement of claim **1** where said firedoor module *i* is physically distinct from said one or more periphery elements of said sub-network *i*.

6. The arrangement of claim **5** where said firedoor module *i* comprises a plurality of firedoor elements, each of which is associated with one of said periphery elements.

7. The arrangement of claim **5** where said firedoor module *i* comprises N_i firedoor elements, each of which is associated with one of said N_i links.

8. The arrangement of claim **7** where each of said firedoor elements that is associated with one of said N_i links is connected to said one of said N_i links.

9. The arrangement of claim **7** where each of said firedoor elements that is associated with one of said N_i links is interposed in said one of said N_i links.

10. The arrangement of claim **5** where at least one of said periphery elements in sub-network *i* is a switch that includes a mirroring port, and said firedoor module *i* is connected to said mirroring port.

11. The arrangement of claim **5** where at least one of said periphery elements in sub-network *i* is a switch that includes a mirroring port, and said firedoor module *i* comprises a plurality of firedoor elements, one of which is connected to said mirroring port.

12. The arrangement of claim **10** where said mirroring port reflects traffic of one of said links that is connected to said switch.

13. The arrangement of claim **10** where said mirroring port reflects traffic of all of said links that are connected to said switch.

14. The arrangement of claim **13** where said mirroring port reflects sampled traffic of all of said links that are connected to said switch on a time multiplexed basis, or of all ports of said periphery element on a time multiplexed basis.

15. The arrangement of claim **10** where said mirroring port reflects traffic of all of said links that are connected to said switch on a time multiplexed basis, or of all ports of said periphery element on a time multiplexed basis, and firedoor module *i* samples traffic received via said mirroring port.

16. The arrangement of claim **1** where said firedoor module *i* that blocks effects of all known malfeasing data aimed to flow into said sub-network *i* through said N_i links by preventing said malfeasing data from passing through said N_i links into said sub-network *i*.

17. The arrangement of claim **1** where said firedoor module *i* includes a firedoor element that is associated with a periphery element of said one or more periphery elements of sub-network *i*, and said firedoor element directs its associated periphery element to nullify effects of, or reject, said malfeasing data.

18. The arrangement of claim **17** where said firedoor element directs its associated periphery element through a control port of said periphery element.

19. The arrangement of claim **1** where said firedoor module i comprises a firedoor element that is associated with a periphery element of said one or more periphery elements of sub-network *i*, and adapted to direct its associated periphery element to block traffic of a particular type.

20. The arrangement of claim **19** where said firedoor element directs its associated periphery element through a control port of said periphery element.

21. The arrangement of claim **1** further comprising a firedoor keeper that is either inaccessible over said network or said other networks, or is accessible through said

network or through said other networks only over a secure connection, by an authorized user, and said firedoor modules of said sub-networks communicate with said firedoor keeper.

22. The arrangement of claim **21** where said firedoor keeper communicates to all firedoor elements and firedoor modules information about detecting presence of known threats and actions to be taken upon discovery of such threats in monitored data.

23. The arrangement of claim **21** where said firedoor keeper directs said firedoor module *i* to block all data that meets preselected criteria.

24. The arrangement of claim **21** where said firedoor module *i* is further adapted to block traffic seeking to flow out of said sub-network *i* when said firedoor module *i* concludes that a likelihood exists that malfeasing data aims to flow out of said sub-network *i*, and to inform said firedoor keeper of said conclusion.

25. The arrangement of claim **21** where said secure connections employ encryption of communication.

26. The arrangement of claim **25** where said firedoor modules of said sub-networks receive from said firedoor keeper, over said secure connections, configuration file updates that provide each of said firedoor modules with information to detect said malfeasing data.

27. The arrangement of claim **21** where said firedoor modules of said sub-networks receive from said firedoor keeper configuration file updates that provide each of said firedoor modules with information to detect said malfeasing data and to take protective action.

28. The arrangement of claim **21** where said firedoor module *i* receives from said firedoor keeper information to direct said periphery switch to reject traffic of a specified type.

29. The arrangement of claim **21** where said firedoor module *i* is adapted to send to said firedoor keeper information about traffic that is indicative of, or may be indicative of, malfeasing data having gained access said sub-network *i*.

30. A method executed in a network that includes a plurality of interconnected switches and processing units connected to said switches, where said network is partitioned into sub-networks that are interconnected via links, said network further including a firedoor element associated with each of said links, said firedoor elements adapted for communication with a firedoor keeper, comprising the steps of:

each said firedoor element:

scanning traffic of its associated link for appearance of any attack from a group of attacks maintained in a patterns file;

taking protective action relative to traffic on its associated link when a attack from said group of attacks appears in said traffic;

reporting to said firedoor keeper when a attack appears in said traffic; and

accepting directives and updates to said patterns file from said firedoor keeper.

31. The method of claim **30** further comprising the step of:

said firedoor keeper:

receiving a report from said firedoor element associated with each of said links that detects appearance of a attack;

analyzing said report to determine whether a directive needs to be sent out, or an update to said patterns file needs to be updated;

creating said directive, or said updated patterns file; and

sending said direction or updated patterns file to said firedoor elements.

32. The method of claim **30** where said step of said firedoor element reporting includes said firedoor reporting to said firedoor keeper when a attack is suspected to be appearing in said traffic.

33. A method carried out by a firedoor apparatus comprising the steps of:

scaning traffic applied to said apparatus to detect existence in said traffic of a pattern maintained in a patterns file;

when detecting a pattern in said traffic that is maintained in said patterns file, it being a detected pattern, retrieving an action from said patterns file that is associated with said detected pattern,

executing said action;

reporting to a firedoor keeper information about said detected pattern when predetermined conditions are met.

34. The method of claim **33** further comprising receiving instructions from said firedoor keeper, and executing said instructions.

35. The method of claim **34** where said instructions are to update said patterns file, or to take immediate action regarding said traffic.

36. The method of claim **33** further comprising a step of analyzing said traffic that is scanned by said step of scanning to identify traffic that meets predetermined suspicion criteria and to trigger (a) said step of executing to take action relative to said traffic, which action relates to said suspicion criteria, and (b) said step of reporting.

37. The method of claim **36** where said suspicion criteria are embedded in a pattern in said patterns file.

38. The method of claim **36** further comprising receiving instructions from said firedoorkeeper to update said suspicion criteria and corresponding action.

39. The method of claim **33** further comprising a step of controlling behavior of a device distinct from said firedoor apparatus, which device is associated with said traffic.

40. The method of claim **39** where said step of controlling behavior of said device comprises a directive to

a. disable all traffic through said device,
b. disable all traffic relative to a source address of said traffic, or relative to destination address of said, or
c. disable all traffic of a selected type.

41. The method of claim **39** where said device is a switch having a plurality of ports, and said step of controlling behavior of said device comprises a directive to couple traffic of a specified one of said ports to said firedoor.

42. A firedoor apparatus comprising:

a firedoors patterns file that maintains a collection of information patterns and associated actions;

a controller that scans traffic applied to said apparatus to detect existence in said traffic of any of said patterns maintained in said patterns file and responds, when existence of a pattern maintained in said patterns file is detected in said traffic, it being a detected pattern, with action specified in said patterns file in association with said detected pattern; and

a communication module for reporting to a firedoor keeper detection of said detected pattern when predetermined conditions are met.

43. The firedoor apparatus of claim **42** where said controller also scans said traffic for patterns that meet predetermined suspicion criteria, and said action module responds, following detection of a traffic pattern that meets said predetermined suspicion criteria with predetermined action that is tailored to said suspicion criteria.

44. The firedoor apparatus of claim **42** further comprising a receiving module, for receiving updates from said firedoor keeper to said patterns file and for installing said updates in said patterns file.

45. The firedoor apparatus of claim **44** where said receiving module receives updates to modules that define operation of said controller and updates processing capabilities of said controller.

46. The firedoor apparatus of claim **44** where said receiving module receives immediate actions to be taken vis-à-vis said traffic.

47. The firedoor apparatus of claim **42** further comprising a control port through which said action module exercises control over a device that is associated with said traffic scanned by said controller.

48. The firedoor apparatus of claim **47** where said control that is exercised by said action module includes directing said device to

a. disable all traffic through said device,

b. disable all traffic relative to a source address of said traffic, or relative to destination address of said, or

c. disable all traffic of a selected type.

49. The firedoor of claim **47** where said device is a switch having a plurality of ports, and said action module directs said switch to make said traffic scanned by said controller correspond to traffic of a specified port of said switch.

50. A method, carried out by a firedoor keeper that is adapted to communicate with a plurality of firedoors comprising the steps of:

receiving from one of said firedoors information about an attempted communication of malfeasing data;

analyzing said information to determine whether no instructions are necessary to be sent, or whether instructions are necessary to be sent to said one of said firedoors, or to all of said firedoors;

when said step of analyzing determines that instructions are necessary to be sent, creating said instructions and sending said instructions to said one of said firedoors, or to all of said firedoors, as determined by said step of analyzing.

51. The method of claim **50** further comprising a step of receiving update data that comprises information about new malfeasing data and actions to be taken when said new malfeasing data is found, and sending said update data to all of said firedoors.

52. The method of claim **51** where said update data is provided by an administrator who is coupled to said firedoor keeper, or provided electronically from a trusted source.

53. The method of claim **50** where said step of analyzing is adapted to determine that said information represents an attack by malfeasing data that has not been previously known.

54. The method of claim **50** where said information arrives at said firedoor keeper in encrypted form, and said step of creating said instructions creates said instructions in encrypted form.

55. A firedoor keeper comprising:

a module for receiving packet data that informs said firedoor of malfeasing data

an controller that

(a) analyzes said packet data to determine whether instructions are necessary to be sent out.

(b) constructs an instructions message when said controller determines that instructions are necessary to be sent out; and

a module for send out said instructions, addressed to a given device, or in a broadcasted to a set of devices.

56. The firedoor keeper of claim **55** further comprising a user interface module for enabling an administrator to assist said controller to analyze said packet data and to construct said instructions.

57. The firedoor keeper of claim **55** further comprising a memory that includes:

a patterns file that said firedoor keeper sends to all firedoors that communicate with said firedoor;

a processing modules collection that that said firedoor keeper sends to all firedoors that communicate with said firedoor;

a patterns file employed by said firedoor keeper;

a processing modules collection employed by said firedoor keeper; and

a information about messages received by said firedoor keeper form said firedoors.